Peter Njogu Kimani

Protection Methods in Traffic Engineering MPLS Networks

Helsinki Metropolia University of Applied Sciences

Bachelor of Engineering

Information technology

Thesis

16th May 2013

Helsinki Metropolia University of Applied Sciences

Author(s) Title Number of Pages Date	Peter Njogu Kimani Protection Methods in Traffic Engineering MPLS Networks 45 pages + 3 appendices 16th May 2013
Degree	Bachelor of Engineering
Degree Programme	Information Technology
Specialisation option	Name of the specialisation option
Instructor(s)	Aydin Karaer, Services Line Manager Puska Matti, Principal Lecturer

The objective of this project was to perform a theoretical review of Multiprotocol Label Switching (MPLS) Traffic Engineering (TE) technology and traffic protection methods in the Traffic Engineering on MPLS networks and implement traffic protection in an ISP's (Internet Service Provider's) network.

The project was carried out first by introducing VPN (Virtual Private Network) and its different categories and modes. VPN is closely related to MPLS. The MPLS-TE was introduced and its operations and protocols. Traffic Protection methods and schemes were also explained in depth. In particular, the focus was on link protection and the different schemes used for local protection. The link protection using FRR (Fast Rerouting) with 1:1 scheme was configured on an ISP network. Testing was done before and after a link failure.

The results from the implementation show that the traffic protection can be used to support the ISP's network failure from affecting the customer's traffic. This can be used to improve the reliability of the ISP's network and reduce delays and communication failure caused by network failures.

Keywords	VPN, MPLS, traffic protection

Contents

Abbreviations

APS	Automatic Protection Switching
ATM	Asynchronous Transport Mode
BFD	Bidirectional Forwarding Detection
BGP	Border Gateway Protocol
CD	Compact Disc
CE	Consumer Edge router
CPVPN	Consumer Provisioned VPN
CSPF	Constrained Shortest Path First
Det	Detour tunnel
ERO	Explicit Route Object
EXP	Experimental
FEC	Forwarding Equivalent Class
FIB	Forwarding Information Base
FRR	Fast Reroute
IGP	Interior Gateway Protocol
ILM	Incoming Label Map
IP	Internet Protocol
IPsec	Internet Protocol Security
IS-IS	Intermediate System to Intermediate System
IS-IS-TE	Intermediate System to Intermediate System Extension for Traffic Engineering
ISP	Internet Service Provider
LAN	Local Area Network
LC-ATM	Label Control Asynchronous Transport Mode
LDP	Label Distribution Protocol
LER	Label Edge Router
LFIB	Label Forwarding Information Base
LIB	Label Information Base
LSP	Label Switched Path
LSR	Labe Switching Router
LTE	Long-term evolution
MP	Merge Point
MP-BGP	Multiprotocol Border Gateway Protocol

MPLS	Multiprotocol Label Switching
NHLFE	Next Hop Label Forwarding Entry
NHop	Next-hop
NNHop	Next-next-hop
OSPF	Open Shortest Path First
OSPF-TE	Open Shortest Path First Extension for Traffic Engineering
P	Provider router
Pde	Primary detour tunnel
PE	Provider Edge router
PHP	Penultimate Hop Popping
PIM	Protocol Independent Multicast
PLR	Point of Local Repair
PPVPN	Provider Provisioned VPN
Pri	Primary tunnel
RIB	Routing Information Base
RNC	Radio Network Controller
RSVP	Resource Reservation Protocol
RSVP-TE	Resource Reservation Protocol-Traffic Engineering
QoS	Quality of Service
S	Stack
SLA	Service-level agreement
SONET	Synchronous Optical Network
TCP/IP	Transmission Control Protocol/Internet Protocol
TDM	Time Division Multiple Access
TE	Traffic Engineering
TTL	Time To Live
VCI	Virtual Channel Identifier
VLSM	Variable Length Subnet Masking
VoIP	Voice over Internet Protocol
VPI	Virtual Path Identifier
VPN	Virtual Private Network
VRF	Virtual Routing and Forwarding
2G	Second Generation
3G	Third Generation

1 Introduction

Today the Internet is the backbone of most communications, a network of computers all over the world for information exchange. The Internet Service Provider (ISP) provides connectivity to individuals and enterprise computers. Thus the Internet can be referred to as public, since the information can be viewed by any Internet user. The principal communication protocol in the Internet communication environment is the Internet Protocol (IP) which uses datagram, also known as network packets in the delivery of data between the source and the destination. The IP network router analyses the destination address of data packets to determine the source and destination. The IP forwarding is based on routing protocols such as Open Shortest Path First (OSPF) and Border Gateway Protocol (BGP). These protocols are designed to forward packets using the shortest path and without considering other factors that may affect the connection such as latency and congestion. Since IP is a connection-less communication protocol, there is a need for a more reliable connection-oriented communication protocol to help with real time communication. [2.]

Enterprises use dedicated lease lines to communicate between different sites of the enterprise. A dedicated lease line provides a high speed connected between locations over the Internet. They are ideal for data, voice and video since they are private lines that carry communication and traffic from the company with a guaranteed level service. [3] The Virtual Private Network (VPN) is used by enterprises to interconnect different business locations over the internet thus emulating a Private Local Area Network (LAN). VPNs have data integrity, confidentiality and authentication. [5, 310]

The Multiprotocol Label Switching (MPLS) was established to overcome some of the shortcomings by IP networks on the ISP network. The MPLS establishes a connection oriented communication over the connection-less framework of the IP network. The MPLS uses Layer 2 (data link layer) information over Layer 3 (network layer) within a particular autonomous system and thus it is referred to as Layer 2.5 protocol. [2; 4]

The goal of the project was to examine different MPLS-TE concepts and services and how they are used in the implementation of network protection in both theory and practice. The aim of the project was to study and gain knowledge of MPLS protection support from theoretical and practical viewpoints. The project implementation concentrated on link protection in an MPLS-TE operator network.

2 Virtual Private Network

The Virtual Private Network (VPN) is a private network that uses a “virtual” connection routed through the Internet from the enterprise private network to a remote site or user. While enterprises use VPNs, they can be ensured security since the data can be encrypted as it goes through the Internet. To be able to access the encrypted data one needs to decrypt it using the right key, which is hard to compute. [5, 310] The VPN connection is also referred to as a VPN tunnel. There are two types of VPN; Site-to-Site and Remote Access VPN.

2.1 Site-to-Site and Remote Access VPN

The Site-to-Site VPN connects two or more offices to each other. The VPN connection over the Internet acts as a WAN (Wide Area Network). Figure 1 below shows a Remote Site connecting to the Corporate Network LAN. [6, 528] Both the Remote Site LAN and the Corporate Network LAN need a VPN Gateway. The VPN Gateways (VPN router) is a connection point that connects two LANs over a non-secure network such as the Internet.

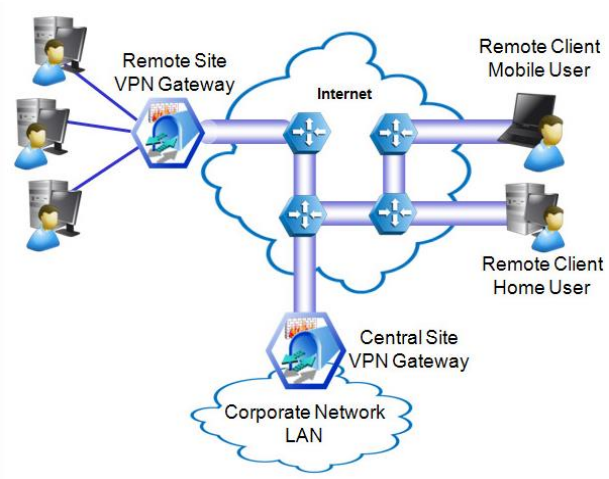

Figure 1. Site-to-Site and Remote Access VPN. Reprinted from HOB (2012) [7]

The Remote Access VPN allows mobile or home workers to connect to the corporate network in a secure way over the Internet. [8, 363-387] Figure 1 above also shows a Remote Mobile User and a Remote Home User connecting to the corporate network.

The users need to have both a VPN client and the company's VPN logging information to be able to connect to the VPN server.

2.2 VPN categories

VPNs are classified as either Consumer Provisioned VPN or Provider Provisioned VPN depending on the endpoint of the tunnel.

2.2.1 Consumer Provisioned VPN

In a Consumer Provisioned VPN (CPVPN) the tunnels are terminated at the Consumer Edge (CE) equipment. The VPN topology is configured and maintained at the CEs. Although the VPN tunnel is routed over the public Internet, the ISP has no idea that the VPN tunnel exists. The secure VPN tunnel can use protocols such as IPsec (Internet Protocol security). [9] Figure 2 below shows an example of a CPVPN.

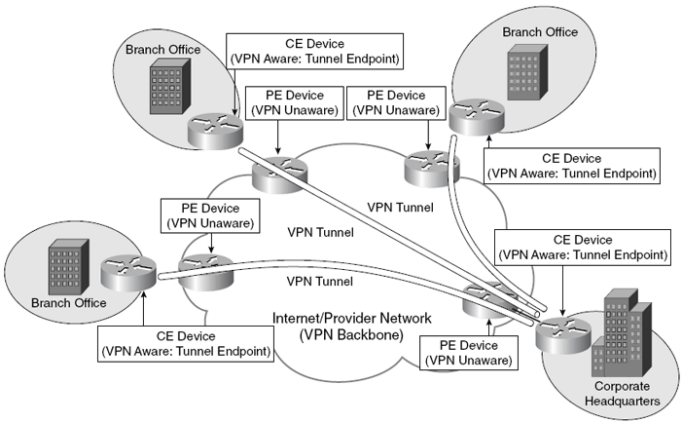

Figure 2. An example of a CPVPN network. Reprinted from Mark L. (2006) [10,13].

Since the CPVPN is configured on the consumer network, the ISP has no control over the CPVPN unless they are commissioned to setup and maintain it

2.2.2 Provider Provisioned VPN

In a Provider Provisioned VPN (PPVPN) the tunnels are terminated at the PE (Provider Edge) device. The network provider is responsible for the configuration and maintenance of the VPN. The consumer is unaware of the VPN tunnel on the provider network. [9; RFC 4026.] Figure 3 below shows an example of a PPVPN.

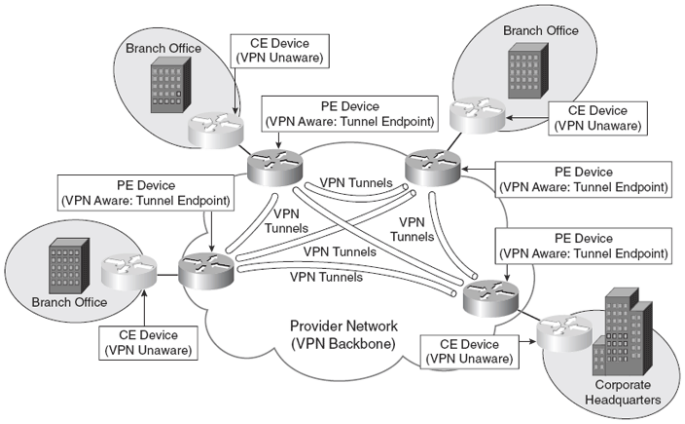

Figure 3. An example of a PPVPN network. Copied from Lewis M. (2006) [10,14].

It is common to have the service provider managing the PPVPN at an extra cost. This makes it cheaper for the enterprise and transfers the risk and workload to the service provider.

In both CPVPN and PPVPN the customer payload carried by the VPN can either be Layer 2 or Layer 3.

2.2.3 Layer 2 VPN

The Layer 2 VPN uses MPLS labels to transport data link layer frames over the Internet on the PPVPN. When the customer devices communicate based on linked layer information such as MAC address and Frame Relay, the provider will need to transport the frames in a way that it will not change during transit. The provider uses a standard MPLS header to encapsulate the frames, thus enabling them to transport Layer 2 data such as ATM (Asynchronous Transport Mode) and Frame Relay. [9; RFC 4664]

2.2.4 Layer 3 VPN

Layer 3 VPN, known as BGP/MPLS IP VPN or MPLS L3VPNs, uses a peer-to-peer model that uses BGP to transport VPN-related data. The Layer 3 VPN peer-to-peer model helps enterprises to cut costs by outsourcing routing services to the ISP. The ISP is also able to add a value-added service such as QoS (Quality of Service) and Traffic Engineering, allowing the network to support more traffic such as data, voice and video. [11.]

MPLS L3VPN uses Layer 3 addressing to interconnect customer devices over the ISP network providing the edge device forwarding customer traffic based on the IP header and the incoming link. The MPLS L3VPN is run as a Provider Provisioned VPN (PPVPN).

2.3 VPN Models

An enterprise's network needs to be interconnected with all the sites. The ISP network is used to make the interconnections using VPN. There are two VPN models that the ISP can use to provide interconnectivity to the customers' network: the overlay VPN model and the peer-to-peer model.

2.3.1 Overlay VPN Model

The overlay VPN is a CPVPN. It uses a point-to-point connection between the customer sites. The connection can either be a point-to-point connection or a virtual circuit. In either of these cases the ISP network acts as a Layer 2 switch between the CE routers. This means that the ISP routers are unaware of the customer routers. As can be seen in figure 4 below, the CE routers form a Layer 3 peering to each other over the ISP network [12, 202-203.]

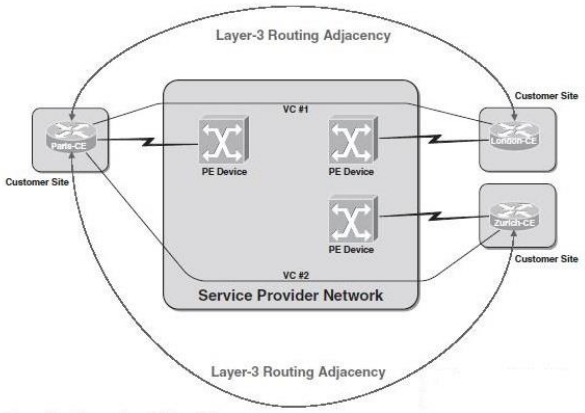

Figure 4: Overlay Model. Copied from Overlay, Peer-to-Peer and MPLS VPN [14]

It can be seen in figure 4 above that the CE routers form peering with the adjacent router over the ISP network.

2.3.2 Peer-to-Peer VPN Model

The Peer-to-Peer VPN model is usually a PPVPN. In the Peer-to-Peer VPN model the CE router peers with a PE router at Layer 3. Unlike the overlay VPN model, in the Peer-to-Peer VPN model the CE router exchanges Layer 3 routing information with the PE router close to it. [12, 203-204.] Figure 5 below shows a CE router a Layer 3 connection with the closest PE router on step 1.

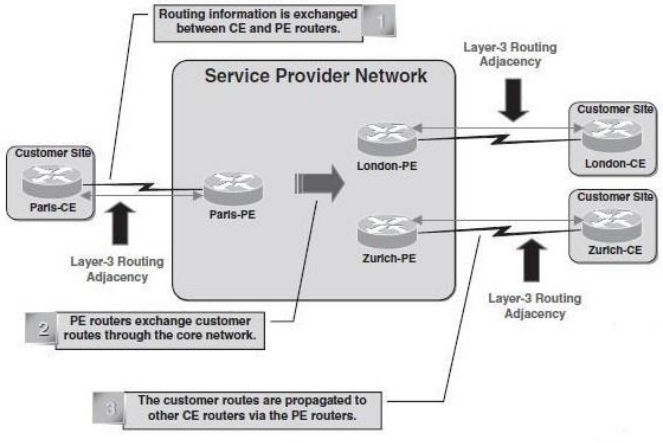

Figure 5: Peer-to-Peer Model. Reprinted from Overlay, Peer-to-Peer & MPLS VPN [14]

In figure 5 above, step 2 the PE router routes the customer data on a hop based on the Layer 3 information. The PE router knows all the routes of the customer sites. On step 3 the PE router exchanges Layer 3 information with the CE router.

Advantages of Peer-to-Peer VPN model over Overlay VPN model include the following:

- Cheaper to the ISP because the routing information in exchanged only on the CE router hence less processing is needed on the PE routers
- It is scalable since new sites can be easily added to the existing network without altering the entire network
- The customer can manage the inbound and outbound bandwidth for each site [24.].

3 Multiprotocol Label Switching

The MPLS is a standard used to speed up the network flow and make management easier. It involves setting up a path for a given sequence of a packet by placing a label on each data packet. This reduces the time to look up for the next hop in the IP tables, so as to forward the data packet. [16.] MPLS is classed multiprotocol because it operates on different Network Layers, Layer 2, Layer 2.5 and Layer 3. It allows most data to be transported using the Layer 2 (switching) rather than the Layer 3 (routing) level. This makes moving data packet traffic faster and the QoS is easy to manage.

The MPLS uses labels to identify virtual links (paths) between distant nodes rather than endpoints. In simple terms a label is a value that prepended to a data packet that informs the network where the data packet is destined. IP networks use the frame mode while the ATM can either use the frame mode or cell mode. [13, 25-28.] Cell mode is becoming absolute.

In the frame model, MPLS works by adding an MPLS header containing one or more MPLS labels to the data packet. This is called a label stack. The MPLS header is placed between the Layer 2 header and Layer 3 header and thus it is called Layer 2½ header. Figure 6 below illustrates an example of a MPLS header. [2.]

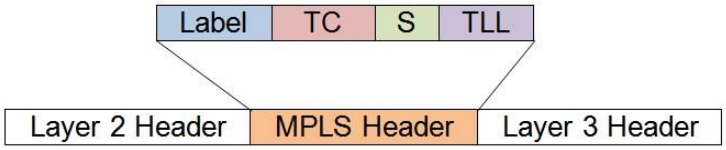

Figure 6. MPLS header

Each label stack entry is made up of 32 bits and contains four fields:

- Label = 20 bits
- TC (Traffic Class) also known as EXP (Experimental) = 3 bits
- S (Bottom of stack) = 1 bit
- TTL (Time To Live) =8 bits.

Label bits consist of encoded information that is used for forwarding the labelled data packet through the network.

TC bits are reserved for experimental use. These bits are also used for QoS and ECN (Explicit Congestion Notification). The ECN is an extension of the TCP/IP (Transmission Control Protocol/Internet Protocol) that allows end-to-end notification of network congestion without dropping data packets.

S bit is the bottom of a stack flag. If it is set, it indicates that the current label is the last in the stack.

TTL bits are propagated from the IP TTL at the ingress LSR and propagated back to the IP packet at the egress LSR. Just as the IP TLL, they are used to prevent loops from creating an infinite data packet storm.

When a tunnel is created between a given pair of edge routers, it is called label stacking. This tunnel may multiplex traffic from different VPNs. Normally two level stack is used where the inner label identify the VPN while the outer label identify traffic that is carried on a common LSP (Label Switched Path) between the edge routers.

3.1 Basic Terminology

Below is some basic terminology used in MPLS:

- **Customer network**: This is the network at the customer's premises. It is configured and managed by the customer.
- **Customer Edge router (CE)**: This is the router at the customer network that connects to the service provider IP/MPLS network.
- **Provider network**: This is the network at the service provider network. It helps to extend the private network of the customer.
- **Provider Edge router (PE)**: This is the last router between the service provider's network and another service provider's network or the customer network, also known as the Label Edge Router (LER). It can be either ingress or egress.
- **Provider router (P)**: This is a transit router inside the service provider's network. It connects one or more PE routers and is also referred to as Label Switching Router (LSR).

- **Label Switched Path (LSP):** Also known as an MPLS tunnel or MPLS VPN (Virtual Private Network). LSP is the route by which MPLS data packets use from the ingress to the egress LER on the network. It is set by signalling protocols such as LDP (Label Distribution Protocol) and RSVP-TE (Resource Reservation Protocol-Traffic Engineering). MPLS allows multiple instances of the routing table within the same router at the same time using the VRF (Virtual Routing and Forwarding) technology. Since each instance is independent of each other, the same or a different IP address can be used without coursing conflict with each other. LSPs are unidirectional and need to be configured on every node. [16; 17; 18.]

3.2 MPLS Mechanisms

The Label Information Base (LIB) is a table maintained by IP/MPLS capable routers. In IP networks, RIB (Routing Information Base) also known as a routing table is a list of routing information in the particular IP network and it is similar to the LIB (Label Information Base) in the IP/MPLS capable routers. LIB maintains tables which store MPLS forwarding information. The MPLS forwarding information includes the port and the corresponding MPLS router label. In IP networks forwarding is based on the destination IP address and the Forwarding Information Base (FIB) while in MPLS it is based on the MPLS label and the Label Forwarding Information Base (LFIB). As in IP network, forwarding in the MPLS network is done hop-by-hop. In the IP network classification in done on every hop, while in the MPLS network it is done only by the ingress LSR. [4, 32.]

3.2.1 IP over MPLS Mechanism

A packet can be allocated one or more MPLS headers but in IP traffic a single MPLS header is enough. The ingress PE router identifies the egress PE to which the traffic is directed to and the LSP. As an IP packet enters the network, the ingress PE router checks the FIB and identifies the route to the egress PE router. It then checks the corresponding destination label in its LFIB and adds an MPLS label to the packet. The process of adding an MPLS label to an MPLS packet is called push. As a packet enters the P router, the router checks its LFIB to determine the next hop. The incoming label is then removed and replaced with the outgoing label and the packet is forwarded. The

removing of the incoming label and replacing it with an outgoing label is called swap. [12, 8.]

At the egress PE router, a normal IP lookup is done to determine which link to forward the data. The MPLS label is then removed and the packet is forwarded as an IP packet. The removing of the label is referred to as a pop. In a large network, the popping of the MPLS label by the PE egress router can slow the network since the process needs more processing power. To reduce the processing needed by the PE egress router, a scheme called Penultimate Hop Popping (PHP) is used. In this scheme, the P router before the egress PE router pops the MPLS label and forwards to the egress PE router as an IP packet. The P router that performs PHP is informed by the neighbouring PE egress router by sending implicit-null as it local label which is to be used by the P router as the outgoing label. The value of this implicit-null is 3. [12, 8.]

The network in Figure 8 below illustrates an example of an IP over MPLS network. An IP packet is sent to from IP Switch 1 to IP Switch 2. Router R1 is the ingress LSR while router R4 is the egress LSR on the MPLS network.

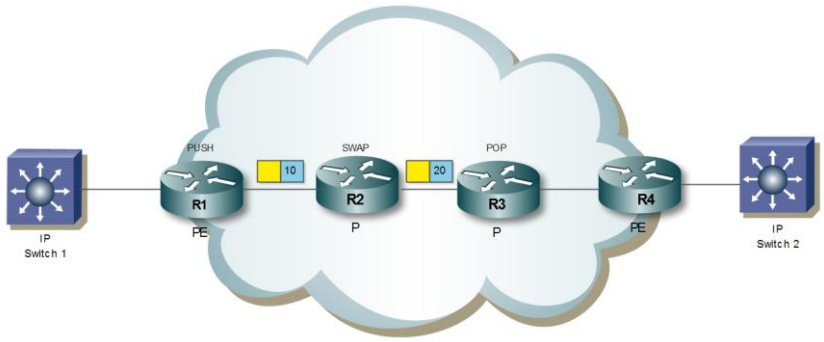

Figure 8. IP over MPLS.

Once the packet gets to the ingress PE router, it is examined by R1, and the destination IP address on the packet, together with other factors such as QoS, decides the FEC (Forwarding Equivalence Class). FEC is a group of IP data packets that are treated the same, forwarded in the same way and in the same path. Normally the data packet is assigned to a FEC based on its network layer destination address. The label is not an encoding of that address. In the MPLS network FEC is performed only on the ingress and egress routers unlike in the IP network where FEC selection is performed on every hop that comes between source and destination. LER (Label Edge Router) is where the agreement on the label to be allocated to the FEC is computed. Each FEC is associated with an appropriate label and forwarding path. There are several models

used to classify traffic by the LER, for example data packet destination address and the port.

The ingress PE router does a table lookup in its Incoming Label Map (ILM) to get the Next Hop Label Forwarding Entry (NHLFE), and determines which P router that packet should be forwarded to. It then pushes a label to the packet and transmits the labelled packet to the next hop router. ILM maps every incoming label to a set of NHLFE and it is used for forwarding packets that arrive as labelled packets. The P router (R2) receives the MPLS packet, performs a table lookup to determine where to forward the packet and swaps the incoming label with the outgoing label, and then forwards the packet.

The P router (R3) can perform the same procedure as the P router (R2) if PHP is not enabled on the egress PE router (R4). In that case the egress PE router (R4) will have to perform both MPLS label popping and IP lookup. For this example PHP is enabled and the local label on the egress PE router (R4) is set to implicit-null. P router (R3) receives the frame, extracts the packet and then looks at the label. Since there is no label for it to forward the packet to, it pops the MPLS label and forwards the packet as an IP packet. The egress PE router (R4) receives the IP packet, and since the MPLS label has been removed by the P router (R3), it only does IP lookup and forwards the packet to the IP Switch. The egress PE can also check for the packets' priorities if they have been set.

3.2.2 MPLS VLANS Mechanism

In an operator's' network, different services and service instances are offered at the same time. This could force the operator to set up different networks for different services and service instances. For example if the operator has a Layer 2 VPN, a Layer 3 VPN and an ATM network, then different networks need to be set and maintained. With MPLS VPN, different services and service instances can be transmitted in the same core network thus, reducing setup and maintenance costs and improving the network scalability and security.

In a network with different services and service instances, a single MPLS header would be insufficient because the egress PE router needs to know which service and which instance for that service the packet belongs to. This can be attained by having two MPLS headers; the outer or top header and the inner or bottom header. These two MPLS headers are called an MPLS header stack. Figure 9 below shows an example of a MPLS header stack. [12, 8]

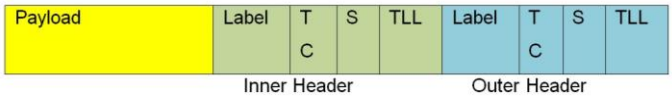

Figure 9. MPLS header stack. Modified from Minei [12, 8.]

The outer header also referred to as ‘transport’ header, is used for transporting the packet from the ingress router to the accurate egress router. The inner header defines the service and the service instance of the packet. The ingress router learns the outer label through either RSVP or LDP protocols. Layer 3 VPNs and BGP-signalled Layer 2 VPNs inner label is lean through BGP while LDP is used in the LDP-signalled Layer 2 transport circuit. [12, 8-9.]

Figure 10 below illustrates an MPLS network with an MPLS header stack. In this example, there are two customers that use this operator’s core network. Customer A’s network is an ATM network while customer X’s network is an IP network. In order for the operator to connect both of these customers’ networks at a minimal cost, they have to use MPLS VPNs.

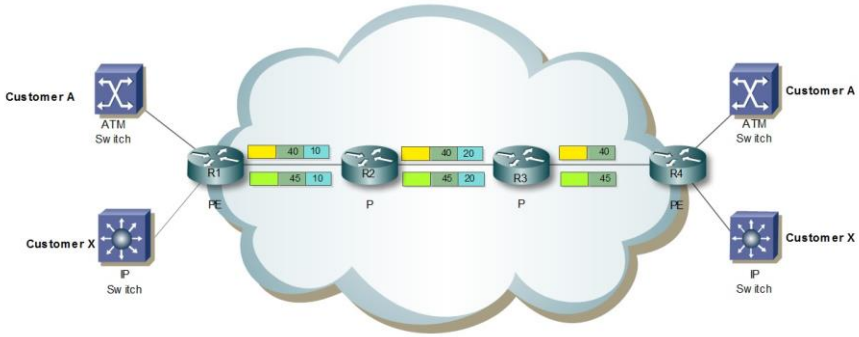

Figure 10. ATM and IP packet with two MPLS headers.

Once a packet from customer A gets to the ingress router, it pushes label 40 that indicates that the packet is of the service ATM and the service instance is customer A. For any packet from customer X, the ingress router pushes label 45 to indicate that it is of the service IP and service instance customer X. The inner label is used to differentiate the two services from each other, identify the source and the destination PEs and is used to specify the LSP to be used.

Both of the packets also get an outer label 10. The P routers between the two PE routers use the outer transport label to execute label lookup; they do not access the inner label. The P router R2 swaps the outer label 10 with the outer label 20. Since PHP is enabled on the egress router R4, the P router R3 pops the outer label and sends the packets with the inner label 40 to the egress router R4. The egress router R4 uses the inner labels to identify the packets for each customer. It pops the inner labels and forwards the packet as they were sent originally, either as an ATM or an IP packet.

One LSP can be used between the ingress and the egress routers to carry all traffic giving MPLS fundamental multiplexing and hierarchical properties because of the ability to stack headers [12, 9.]. This is important in an operator's network since the network is used to transmit different traffic modes for different customers.

3.3 LSP Selection

An LSP selection has to be defined before an LSP can be created. There are two methods in the selection of LSP: hop-by-hop and explicit routing.

3.3.1 Hop-by-Hop Routing

In hop-by-hop the routers send requests, and distribute and release label binding information. The routers discover neighbouring routers and establish a session with the peer. In an IP network, as a data packet arrives to a router, the router looks at the destination address on the IP header, performs a router lookup in its routing table and forwards the data packet to the next hop. In an MPLS network, as the data packet arrives at a router, the router looks at the incoming label, looks up in the label in a table and forwards the packet to the next hop. [16.]

3.3.2 Explicit Routing

Explicit routing has similarities with source routing since source routing allows the sender of the data packet to specify the route the data packet will take through the network. In explicit routing the entire list of nodes in which the data packet will pass by is specified in advance. This router is based on the overview of the whole network and additional constraints such as QoS, and it could be optimal or not. This can be denoted as Constraint-Based Routing.

To ensure QoS, resources could be reserved hence permitting traffic engineering to be deployed in the network to optimize bandwidth usage. [19.]

4 MPLS Protocols

There are three signalling protocols in MPLS that are used to distribute the MPLS labels namely LDP (Label Distribution Protocol), MP-BGP (Multiprotocol Border Gateway Protocol) and RSVP-TE (Resource Reservation Protocol-Traffic Engineering). Since LDP and RSVP-TE are signalling protocols and are incapable of routing, an IGP (Interior Gateway Protocol) is required for the transmitting of topology information to all the routers in the network. The Link State Protocol is the only protocol that can perform this task. [18,255.]

In a Link State protocol, each router creates a packet (Link State Packet) which is flooded to the other routers in the network. On receiving this Link State Packet, the routers compute the Shortest Past First (SPF) algorithm to the other routers in the same network. Once this network is created, the topology can be called a Shortest Path Tree. There are two link protocols for traffic engineering:

- Intermediate System to Intermediate System (IS-IS) Extensions for TE
- Open Shortest Path First (OSPF) Extensions for TE.

OSPF and IS-IS are both link-state routing protocols since they distribute routing information and calculate routes between all routers in the administrative domain. Each router views the network separately, this making any incorrect information from a single router not affecting the network. The following information is needed for the routers to make consistent routing decisions: [18, 226-227.]

- Immediate neighbour connectivity
- recognize other routers and network through LSAs
- the best path to each destination

The IS-IS-TE and OSPF-TE protocols are classless protocols that support VLSM (Variable Length Subnet Masking) and maintain a link state database from the Dijkstra-based SPF algorithm that computes the shortest-path tree. Hello packets are used for forming and maintaining adjacencies. A designated router is selected to represent on broadcast networks.

OSPF-TE is an extension of OSPF which also runs TCP/IP on the signalling control network. It is a control plane protocol used by network operators to manage MPLS packets. It advertises traffic engineering information to all the routers that are part of the same administrative domain. Changes to the network resources, such as bandwidth, links and nodes disruption and/or failure, are instantly shared to all the routers in order to manage the network with fine and accurate information. It is the most common IGP protocol in the operator's network. OSPF-TE supports both LDP and RSVP-TE.

4.1 Label Distribution Protocol

The Label Distribution Protocol (LDP) is an MPLS protocol that enables routers participating in the MPLS network to exchange label mapping information. It can be used in both Layer 2 and Layer 3 VPNs. The exchange of information is bi-directional. Once the mapping information is exchanged, a session is formed between the LSRs. The LSRs in an LDP session are known as LDP peers. LSP databases that are used for forward traffic on an MPLS network are built and maintained by the LDP. [RFC 5036; 26, 34]

Each LSR creates a local label binding for each prefix in its IP routing table which is in turn distributed to each of the neighbouring LSRs. The incoming label is the local label of the LSR. An LSR can have one label per prefix or one label per prefix per interface. However it can have more than one remote binding since there is usually more than one adjacent LSR for each LSR. The LSR sets up its Label Forwarding Information Base (LFIB) based on the information it receives from the downstream LSR, which is the next hop in the routing table for that prefix. [26, 34-35]

Below is a list of the main functions of the LDP:

- Discovery of neighbour LSRs
- Establishment of session
- Maintenance of the session
- Advertisement of the label
- Notification.

For MPLS to work, the LDP needs to establish and maintain a session. The LDP starts a Hello Adjacency after both the LSR have sent and received hello messages. There can be a directly connected neighbour or a non-directly connected neighbour. The non-directly connected LSR can be two or more hops away. The hello messages sent are determined by the neighbour's connection type. For a directly connected neighbour, multicast UDP hellos are used. This method is known as basic discovery mechanism. The other method, an extended discovery mechanism is used for non-directly connected LSRs and uses targeted UDP hellos. [27; 18, 73-76.]

The LSR checks the LDP ID and the LSR with a higher LDP ID becomes the active LSR while the other one become the passive. Then the LSR initiates a TCP session. After the TCP session is established, an LSP is initiated by exchanging session parameters. The session is said to be established once both the LSR are able to exchange Keep-alive messages. These Keep-alive messages are the ones used in maintaining the LDP session. Once the LDP session is started, the LSR starts to exchange the label bindings. [27; 18, 73-76.] Figure 11 below shows LDP label distribution and assignment.

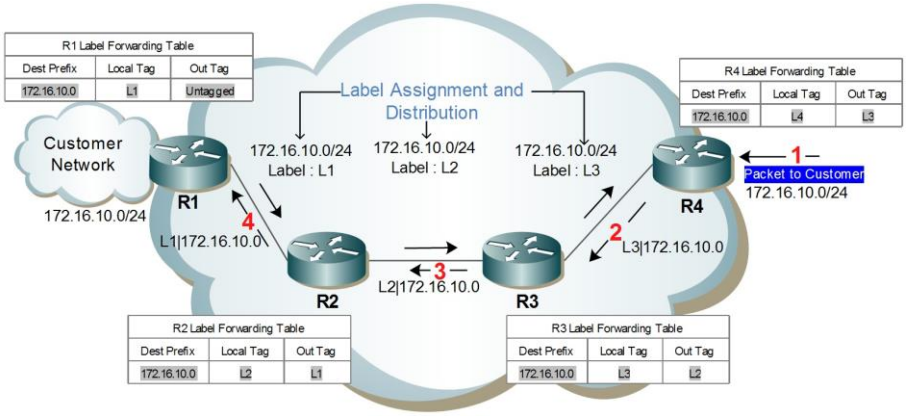

Figure 11: MPLS LDP distribution. Adapted from Lancy L. (2005) [25]

In figure 11, there are two edge LSRs (R1 and R4) also known as PE (provider edge) routers and there are two provider LSRs (R2 and R3), also known as P (provider) routers. LSR R1 creates a local label L1 and advertises it to LSR R2. LSR on the other hand LSR creates a local label L2 and advertises it to the neighbouring LSRs R1 and R3. This happens to both LSRs R3 and R4. Since the exchange of the information is bi-directional, the same process happens from LSR R4 to LSR R1.

Figure 11 shows an IPv4 packet destined to the customer network entering the MPLS network ingress LSR R4 where it is assigned the label L3 and switched to the next LSR R3. This process of adding the label is called PUSH. When the packet gets to LSR R3, the LSR swaps the incoming label L3 with the outgoing label L2 and the packet with the new label is switched to the next LSR. The same process happens on LSR R2. When the packet gets to the PE router LSR R1 the label on the packet is dropped and it becomes an IP packet. This can be seen from the forwarding table of R1 in figure 11.

4.2 Multiprotocol Border Gateway Protocol

Multiprotocol Border Gateway Protocol (MP-BGP) also known as Multiprotocol BGP or Multicast BGP is an extension of Border Gateway Protocol (BGP) that allows different types of addresses (address families) to be distributed. Unlike BGP which supports only IPv4 unicast addresses, MP-BGP supports both IPv4 and IPv6 addresses and both unicast and multicast variants of each address category. [20.] It is used in MPLS and IP VPNs (Layer 3 VPNs).

MP-BGP allows information about the topology of IP multicast-capable router to be exchanged separately from the topology of normal IPv4 unicast routers. It allows a multicast routing topology different from the unicast routing topology. Even if MP-BGP enables the exchange of inter-domain multicast routing information, other protocols such as Protocol Independent Multicast (PIM) family are needed to build trees and forward multicast traffic. [20.]

PIM provides a one-to-many and many-to-many distribution of data over an LAN (Local Area Network), WAN or Internet. PIM depends on information from the traditional routing protocols such as RIP (Routing Information Protocol), OSPF (Open Shortest Path First), BGP and Multicast Source Discovery Protocol since it does not include its own topology discovery mechanism. [21.]

4.3 Resource Reservation Protocol – Traffic Engineering

Resource Reservation Protocol (RSVP) is a Layer 4 (Transport Layer) Protocol designed for resource reservation on a network and supports QoS, optimisation and protection for an integrated services Internet. The RSVP is used by a host or a router to request for QoS for an application data stream or flow from the network. [RFC 2205].

RSVP is not a routing protocol but it operates over the IP network and can support both multicast and unicast data flow. [28,185-189.] It uses Downstream-on-Demand (DoD) label distribution since the labels are advertised from tail end LSR to head end LSR, hop-by-hop. [18, 280-291.]

The RSVP was extended in MPLS Resource Reservation Protocol–Traffic Engineering (RSVP-TE) to enable the setup of LSPs that can be used for Traffic Engineering (TE) in MPLS networks. The LSP setup is configured on a head-end device and initiated by a TE application. The LSP tunnel can be set up as either explicit or dynamic. In explicit, all the LSRs that the tunnel must be routed on must be specified until the tail LSR. To specify the LSRs one can use the LSR's ID or the IP address. In dynamic only the tail LSR is configured on the head LSR and the will be calculated on the head end LSR using the MPLS-TE database learned from either OSPF or IS-IS. [18, 269.] Figure 12 below shows an example of LSP setup taking place.

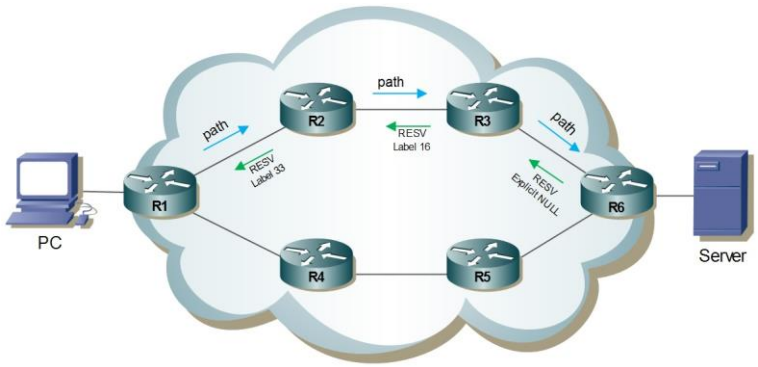

Figure 12: LSP setup in RSVP-TE

A multimedia application in the PC wants to transmit traffic to the Server. The head LSR (R1) identifiers this as a TE application and sends a PATH message having a Labe Request Object (LRO). [18, 280.] Once the tail LSR (R6) receives the Label Request, it sends two local decision modules:

Admission control module: It determines if the node has enough available resources to supply the requested QoS.

Policy-control model: It checks whether the requester has the administrative rights to make the reservation.

In case any of these checks fails, an error notification is returned to the application that made the request. If both checks succeed, the RSVP program configures the packet classifier in the node to determine the data packet that receives the QoS. The RSVP also sets the schedule for providing the QoS on the outgoing link. This creates a reservation state in the node. R6 allocates a label to this tunnel and advertises it to R3. R3 assigns this as the outgoing label in the LFIB for the given TE tunnel. R3 also allocates a label for this TE tunnel and sends it to in a Label object in the RESV message to R2. This becomes the incoming label for the TE tunnel. This continues until the RESV message is received by the head LSR of the TE tunnel. [18, 280.]

Once the RESV message is received by the LSR, the TE tunnel is created and the application on the PC can communicate with the server. The reservation has to be refreshed periodically since RSVP is a soft-state protocol. The RSVP will go down if either it is explicitly removed from the network or if it times out. [13,139]

The main functions of RSVP-TE include end-point control that establishes and maintains the TE tunnels between two end points. The link management that runs between the end point to manage the TE links, and fast reroute (FRR) used for fast traffic recovery once a link or router fails for mission critical services. [28,189: 13,139] The fast reroute is used in traffic protection.

4.4 Comparison between LDP and RSVP-TE Protocols

Looking at different features of LDP and RSVP-TE, table 1 below can be used to bring out the main differences and aid a service provider to select the signalling protocol depending to the needs of his enterprise and the resources available.

Table 1. Comparison between LDP and RSVP-TE

	LDP	**RSVP-TE**
Simplicity	Simple	Complex but better control
Topology	Multipoint-to-point	Point-to-point
Convergence	100s ms – 10s ms (topology dependant)	≤ 50 ms possible
QoS	Relative	Guarantee possible
Protection	Not applicable	Guarantee possible
Bandwidth reservation	Not applicable	Guarantee

By simply turning on LDP on the router/interface, labels are immediately advertised for each route to all the LDP peers. LDP creates a full mesh LSPs between all the nodes configured with LDP which are in the same administrative domain. This means the routing tables on the routers will contain information not needed, thus increasing the lookup time and increasing the required processing in the router. LDP can perform well only in a small network. In RSVP-TE, each LSP should be manually configured. In large network it is time consuming to set up and maintain these LSPs.

QoS on LDP is limited since only the EXP bit can be used to incorporate relative QoS using LDP. This means it is possible to prioritize and apply schedule queuing on LDP. RSVP-TE can guarantee the requested bandwidth. It is also possible to protect both the nodes and the link in RSVP-TE using FRR (Fast Reroute) which can be configured to bypass a failure in 50 ms or less. This increases the level of QoS on RSVP-TE.

5 Traffic Protection

In many enterprises, the network should be available at all times. Some services such as video-telephony, VoIP and media streaming do not tolerate data loss and/or delays, which is not always the situation. From time to time there happens to be a network failure and data is lost. Because of this, the traffic on the MPLS network needs to be protected against network failure. Traffic protection is the fast restoration of the network resources to ensure minimum data loss. Resources can be either logical (LSP) or physical (the nodes or the links). Network failures can be triggered by different reasons such as a loosely connected cable, router crashes, power loss, cable or fiber cuts, to mention a few. A network failure can be classified as either a link failure or a node failure.

A link failure can be triggered by a cable or fiber cut, a loosely connected cable or a number of other factors that connect to the LSR router, together leading to loss of a data packet in between the LSR. A node failure will occur when an LSR router fails to function normally. This can be a result of different factors such as power loss to the LSR router, an LSR router system crash, and a human error such as an accidentally turning off the router. [13,291-292.]

Before MPLS, a network failure existed but the IGP was the main protocol that the network administrators used to router around the failure to the working part of the network. Below are some things that IGP was inept to handle well: [13,291-292.]

- Delay between network interruption and network re-routing
- Network congestion until the new route is created
- Data lost during the failure affect sensitive data such as voice and video.

IP networks running a synchronous optical network (SONET) can use Automatic Protection Switching (APS) to help in fast network recovery. APS switches from the active to standby link within 50 ms when a link goes down. Although this time may be reasonably acceptable, a data packet may still be lost since the APS have to wait until the other end link comes up. ASP is also not commonly used since not all equipment support it, thus resulting in additional costs. [13,292.]

In an MPLS network fast restoration of the network resources is used to protect the network from data loss. Protection can be implemented on RSVP-TE enabled MPLS networks and can be divided into:

- Path Protection (End-to-end protection)
- Local Protection
    - Link protection
    - Node protection.

This report will focus on link protection on an RSVP-TE network.

Before the network can be protected, first a way to notify it that there is a failure has to be established. The BFD (Bidirectional Forwarding Detection) protocol is used to detect the status of the link or node between two locations. BFD sends hello messages to the next hop and waits for a reply. BFD by default can detect a failed connection in 100 ms but it is possible to configure it to have as low as 10 ms detection time. [12, 69.]

5.1 Path Protection

With MPLS support of Traffic Engineering, it is possible to enable a backup LSP for the primary LSP. Backup LSP is also referred to as secondary or standby path. The backup LSP has the same features such as bandwidth and source-destination pair as the primary LSP. This ensures that the network characteristics remain the same, no matter if the LSP in use is the primary or backup LSP. Path protection provides an end to end failure recovery mechanism for the MPLS-TE tunnels. One or more LSPs are established in advance, which provides failure protection for the protected LSP. Links should not be share between the primary and backup LSP since failure to the shared link or node would affect both the LSPs. Figure 13 below shows an example of a network with a primary and a backup path from R1 to R6.

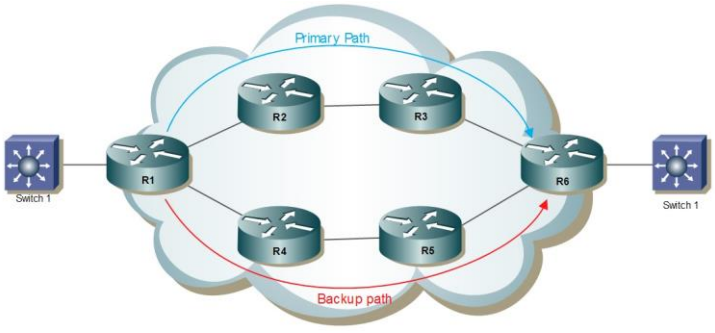

Figure 13. Primary and backup path in path protection

As can be seen in figure 13 above, the primary path from R1 to R6 is R1-R2-R3-R6 while the backup path is R1-R4-R5-R6. In this case if the primary path fails, the traffic will be immediately temporarily switched onto the backup LSP.

5.2 Local Protection

In local protection only a segment of the primary LSP is protected. Here the backup LSP is routed round the failed node or link and the primary LSP that could have gone through the failed link or node is encapsulated in the backup LSP. Since only a segment of the primary LSP is protected, it is important to protect the most important nodes and/or links; such as those that forward data with high priority such as voice and video since they do not allow interruption from failure of the node and/or link. Also to consider is the kind of service-level agreement (SLA) the provider has with the customer. If the customer's SLA is of importance, for example the bank, then one needs to consider the kind of protection which will be applicable for the said customer.

Advantages of Local protection over Path protection include the following:

- Faster failure recovery
- Scalability.

5.2.1 Local Protection Terminology

PLR (Point of Local Repair) is where the backup starts, also known as the head end. In figure 14 below, R2 is the Point of Local Repair.

MP (Merge Point) is the point where the backup path ends and connects back to the network which was part of the primary path. In figure 14 below, R3 is the MP to backup path 1 while R4 is the MP to backup path 2.

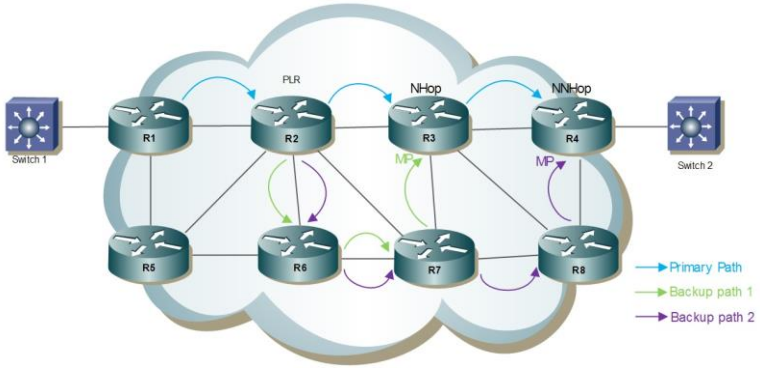

Figure 14. Elements of a local protection.

NHop (Next-hop) is a router one hop away from the PLR. In figure 14 above, R3 is the NHop on the primary path.

NNHop (Next-next-hop) is a router two hops away from the PLR. In figure 14 above, R4 is the NNHop on the primary path.

In some documentation, backup path maybe referred to as a backup tunnel or either an FRR tunnel or bypass tunnel.

5.2.2 Protection Schemes

There are different protection schemes in use as explained below:

1+1 protection

In this scheme a single active protection path is used to protect the MPLS packet. The bridge at the head router is permanent. The packets are transmitted through both the LSPs and the egress router selects the better of the two traffics. In case of a failure, the destination router switches to the active LSP. The disadvantage of this protection is the misuse of the bandwidth since traffic is broadcasted on both the LSPs and no other traffic can use them. [RFC 4427.] Figure 15 below shows an example of the 1+1 protection scheme.

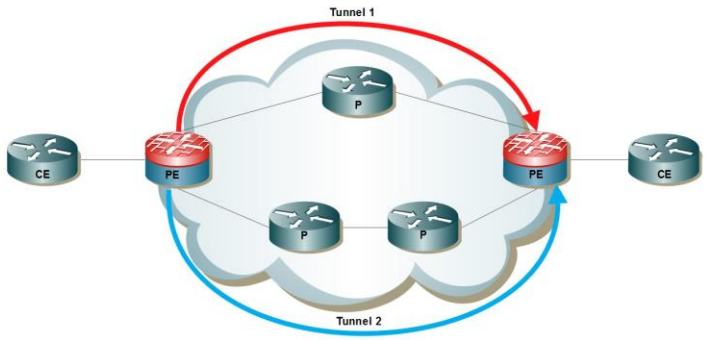

Figure 15. 1+1 protection scheme

In the example illustrated in figure 15, both the tunnels have the same priority configured on them. Traffic is transmitted on both the links but on getting to the right PE router, the router selects traffic from one of the links. The traffic from the other link is dropped. In case tunnel 1 is selected to transmit traffic, tunnel 2 will still transmit the same traffic and it will be selected only if tunnel 1 fails.

1:1 protection

For 1:1 protection (one-to-one protection) there is one primary LSP and one backup LSP. Unlike the 1+1 protection, the bridge at the head router is not permanent. When the primary LSP fails, the backup LSP takes over. During normal operation, low priority traffic can be sent through the backup LSP. This reduces the misuse of network resources. [12, 77-81.] Figure 16 illustrates a 1:1 protected network.

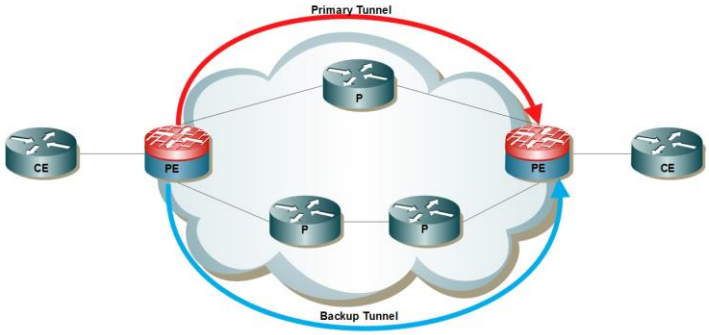

Figure 16. One-to-one protection scheme.

In the example illustrated in figure 16, traffic is transmitted over the primary tunnel during a normal network operation. In case of a failure, the backup tunnel is used. Since the backup tunnel is used only during a network failure, it can be used to transmit other low priority traffic during normal network operation.

N:1 (N > = 1) protection

N:1 protection is also known as many-to-one protection or facility backup or protection. This scheme has N primary LSPs and only one backup LSP. High priority traffic is sent through the primary LSPs. No traffic or low priority traffic is sent through the backup LSP. In case any of the N LSPs fails, the traffic will be rerouted to the backup LSP. This protection does not misuse network resources such as bandwidth since the backup LSP is shared by many primary LSPs and it can still be used to transmit other data when the network is working normally. The disadvantage of using this protection comes in when the number of protected LSPs is big. In case more than one LSP fails, the backup tunnel will support a limited number of traffic depending on available resources and traffic from the other LSP will be dropped. [12, 75-76; RFC 4427] Figure 17 below shows an example of N:1 protection.

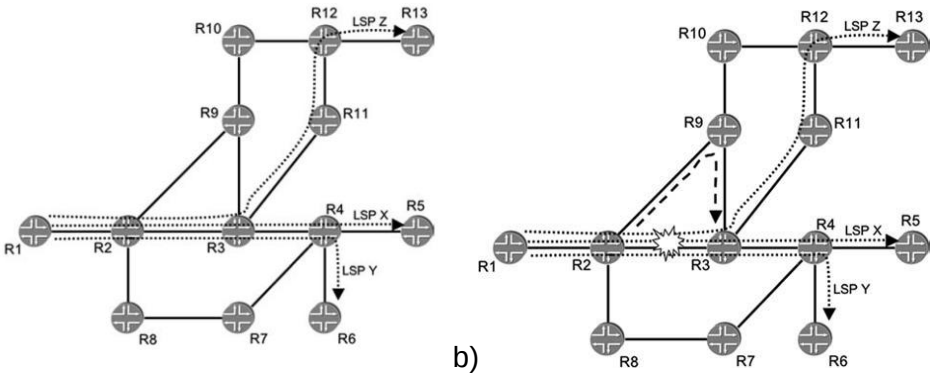

Figure 17. N:1 protection scheme. Reprinted from Minei I [12, 75-76.]

In part a) of figure 17, the network is working normally. The link R2-R3 is shared by all the tunnels. In case of a link failure, as illustrated in figure 17 b), traffic is transmitted through the bypass tunnel R2-R9-R3. This shows that this bypass is shared by all the three tunnels. It is configured with enough resources to support traffic from all the links.

N:M (M > = 1 and N > = 1) protection

In this scheme there are N primary LSPs that carry normal traffic and M backup LSPs that may carry extra (low priority) traffic. In a normal operation, low priority traffic can be sent through the backup LSPs while the high priority traffic is sent through the primary LSPs. Since there are more backup LSPs, in case of a multiple LSPs failure the traffic will be sent through the backup LSPs until the number of failed LSPs is greater than the backup LSPs or the available resources are exhausted.

5.2.3 Link Protection

Link protection is the ability to protect traffic forwarded on an LSP in case the LSP fails. To protect this LSP against a failure, a backup LSP is created that forwards traffic around the filed LSP. This backup LSP is referred to as a detour in case of a 1:1 (one-to-one) protection and a bypass in case of a N:1 (many-to-one) protection. FRR is used to allow the protection of TE tunnels, thus ensuring important data flow through the network even when an LSP fails. [13,299-230] Figure 18 below shows a network with a primary link protected.

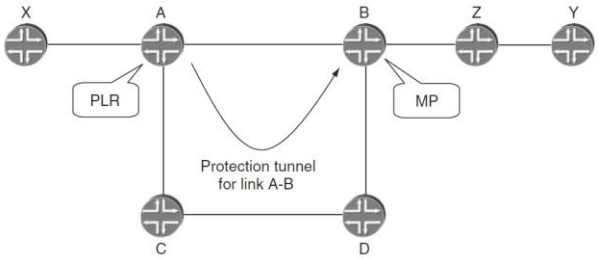

Figure 18. Link protection. Reprinted from Minei I [12, 82.]

The link A-B is protected by the backup tunnel A-C-D-B. When communication between X and Y fails between the link A-B, the data will be redirected through the backup tunnels and the communication will not break. For the customer there may be no effect on the communication, since only the operator knows about the detour. In figure 18, the only protected link is A-B. This means that if it happens that any other link fails between X and Y, there will be a total network failure on the network. This is a good example of a 1:1 protection.

Before a failure occurs, the backup should be ready to transmit traffic when the failure occurs. This means computation of the backup path should be done well before and signalled. The PLR, MP and all the nodes in between should know the forwarding state. This forwarding state should be at the head and tail router for the traffic to be transmitted through the backup. [12, 82-83.]

The forwarding state is the technique used to direct the traffic round a failed link through the backup tunnel and back to the main LSP. The techniques are differentiated by how the traffic gets back to the main LSP at the MP router. These forwarding states are one-to-one (1:1) backup and facility (N:1) backup.

One-to-one backup

In 1:1 backup, the traffic gets to the MP router with a different label than the one in the main LSP. [12, 85] It can be illustrated as in figure 19 below. The main path is X-A-B-Z-Y while the backup path is X-A-C-D-Z-Y, thus meaning that the protected link is A-B.

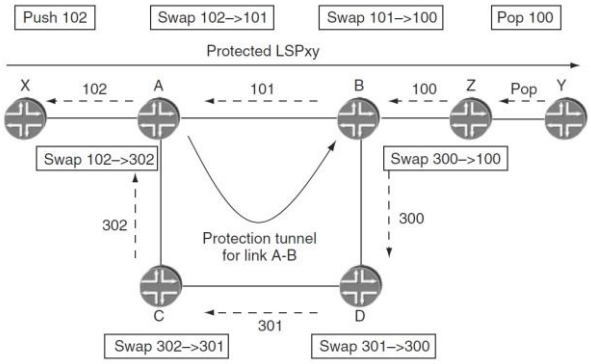

Figure 19. Traffic over the primary link in a 1:1 network. Reprinted from Minei I [12, 86.]

When a packet is being transmitted from X to Y, router X pushes label 102 to the packet. This label will then be swapped with label 101 in router A and with label 100 in router B. Router Z will pop the label and the packet will be transmitted in its original state to router Y.

In case of a failure on link A-B, a different LSP will be followed from the main LSP, or otherwise there will be data loss. In figure 20 below, link A-B has a problem and the data is sent though the backup link.

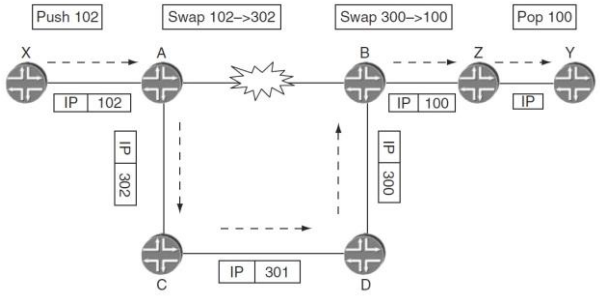

Figure 20. Traffic over the backup link in a 1:1 network. Reprinted from Minei I [12, 86.]

In this case, when the packet arrives at router X, the label 102 is pushed into the packet. In router B the label is swapped with label 302 and to be sent to router C. Router C and router D will swap the label with label 301 and 300 respectively. The packet arrives to Router B with label 300 which is different from the label that the same label could be having in case it used the primary link. Router B swaps the label with label 100. Router Z pops the label and sends the packet to router Y.

Facility backup

In N:1 backup, the packet will get to the MP router with the same label as it could have if it was using the primary link. This is because the MP router is configured with an implicit null and which also helps the router to protect more than one link. [12, 83-84] Figure 21 below shows a network with a N:1 backup enabled. The primary LSP is X-A-B-Z-Y and the backup LSP is X-A-C-D-B-Z-Y. Link A-B is the protected link.

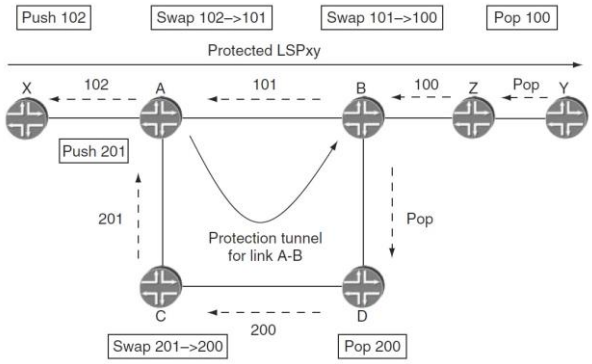

Figure 21. Traffic over the primary link in a N:1 network. Reprinted from Minei I [12, 84.]

When a packet is been transmitted from X to Y, router X pushes label 102 to the packet. This label will then be swapped with label 101 in router A and with label 100 in router B. Router Z will pop the label and the packet will be transmitted in its original state to router Y. Figure 22 illustrates a link failure on link A-B.

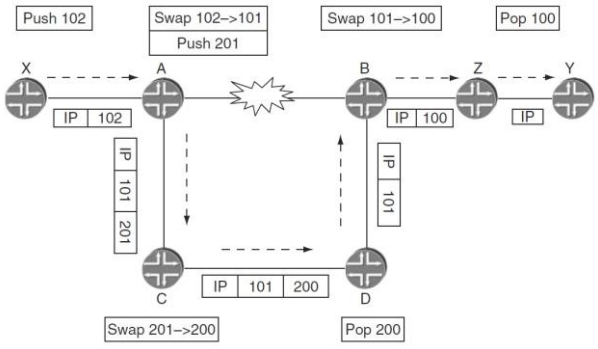

Figure 22. Traffic over the backup link in a N:1 network. Reprinted from Minei I [12, 85.]

As the packet joins the network, router X will push label 102 to the packet. Router A will push the label 201 on top of the primary label. This means that this packet will be having two labels at this time. Router C will swap the outer label with label 200. Router

D will pop the outer label and will forward the data with the primary label, label 100 to router B. As it can be seen, this is the same label the packet could be having if it used the primary LSP only that it is getting to router B from a different interface. Router B will swap label 101 with label 100. Router Z will pop the label and forward the packet to Router Y.

5.2.4 Node Protection

In node protection, one or more nodes are protected to prevent data loss or delays if it happens that the given node fails. When a node is protected, it means that also the links that connect to that node will be automatically protected. Figure 23 below shows an example of node protection.

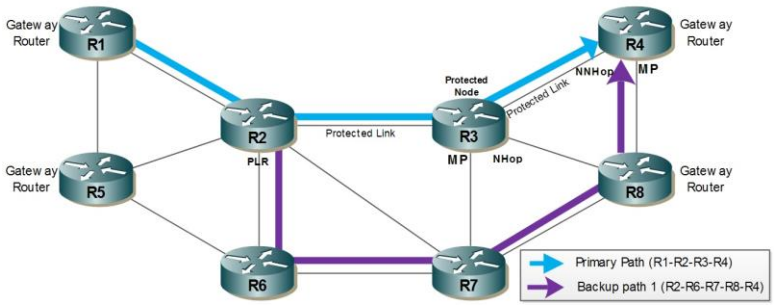

Figure 23. Node protection. Adapted from Osborne E, Simha A. [13]

In the example in figure 23 the protected node is R3. If it happens that this node fails, the traffic will be transmitted through the backup tunnel. In a normal network operation, the backup tunnel can be used to transmit low priority data. The two links connected to R3 (R2-R3 and R3-R4) are also protected since if no connection update is received from R3, the traffic will also be transmitted through the backup tunnel.

6 Implementation of FRR with 1:1 Backup Protection

This final year project was implemented at the Tellabs Laboratory branch in Espoo with real Tellabs equipment. Tellabs is a telecommunications company that designs and manufactures equipment for the service providers. It was established in 1975 and has its head office in Chicago, USA. The name Tellabs combines the idea of telephones and laboratories.

The Tellabs 8600 series routers were used for the implementation for their availability at Tellabs Laboratory and support of both the study technology and ISP's network. The Tellabs 8600 supports all the operators' media and technology needed for second generation (2G), third generation (3G), LTE (Long-term evolution) and LTE-Advanced evolution (IP/MPLS, TDM (Time Division Multiple Access), ATM and Frame Relay). For this reason, it is one of the most used routers in the operators' networks.

A sample operator's network was used for the implementation. This project mainly focused on MPLS protections. Between the LDP and RSVP signalling protocols, only RSVP supports traffic engineering. Traffic engineering supports protection which is why RSVP-TE was selected for the implementation of the project.

One-to-one and facility protection schemes are the most used protection schemes in a provider network. The Tellabs 8600 supports both the technologies. A ready topology was offered at Tellabs Laboratory. One-to-one protection scheme was the most suitable for this topology. In the project, link protection using FRR with 1:1 backup was used on the RSVP-TE network.

6.1 Network Topology

The main focus was the implementation of link protection in the MPLS network using the TE technology. The topology was ready built at the Tellabs Laboratory, and it reflects a typical operator's network. Figure 24 below shows the topology used for the implementation.

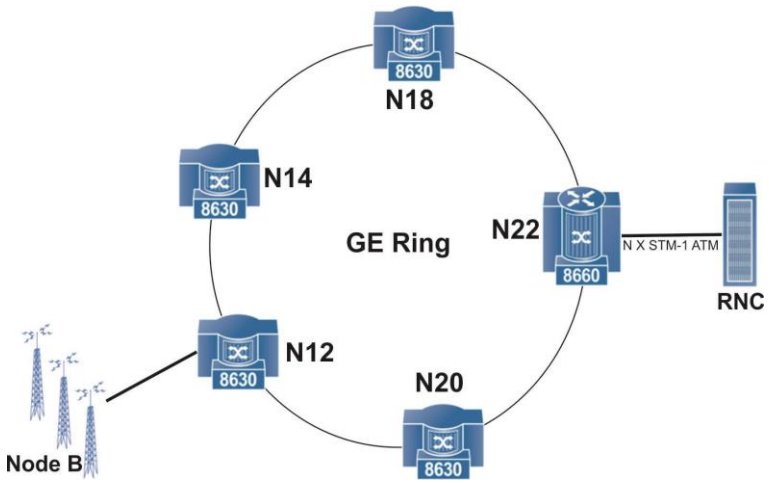

Figure 24. Network topology.

The network supported a Node B and an RNC (Radio Network Controller). The Node B was connected to N12 which was the ingress LSR of the MPLS network. N22 was the egress LSR and was connected to the RNC. This forms a ring network with two possible MPLS routes; N12-N20-N22 and N12-N14-N18-N22. The 3G network IP-based traffic used for data and ATM based traffic used for voice to get to the MPLS network from the Node B. In N12 IP-packets and ATM cells are labelled and transmitted through the network as MPLS packets via MPLS based Layer 2 and Layer 3 VNPs. In N22 the labels are removed and they are transmitted again as IP packets and ATM cells towards the RNC.

6.2 Implementation and Configuration

The IGP protocol used in the project was OSPF-TE. OSPF-TE is the preferred IGP protocol over IS-IS-TE on the ISP's network. Basic IGP, ATM-based Layer 2 VPN and IP-based Layer 3 VPN are not shown in this work since the implementation of RSVP-TE protection is not bound to VPNs.

An RSVP path had to be configured to enable MPLS-TE traffic between N12 and N22. In the topology the path was named N12toN22_Forward_Tunnel_Path. In RSVP an end-to-end path has to be configured on the ingress LSP because LSPs are unidirectional. In listing 1 below, the name of the RSVP path can be seen.

```
N12# show router rsvp
rsvp-path N12toN22_Forward_Tunnel_Path
    10.123.100.20 strict
    10.123.100.22 strict
rsvp-trunk N12toN22_Forward_Tunnel
    primary path N12toN22_Forward_Tunnel_Path
    primary label-record
    primary elsp-preconfigured
    primary fast-reroute protection one-to-one
    from 10.123.100.12
    map-route 10.123.100.22/32
    to 10.123.100.22
```

Listing 1. RSVP configuration in N12

RSVP uses either the CSPF (Constrained Shortest Path First) algorithm or ERO (Explicit Route Object) to determine how traffic will be routed through the network unlike LDP which is restricted to using the configured IGP's shortest path through the network. The ERO limits LSP routing to a specified list of LSRs. The ERO needs to be configured because by default the RSVP path is determined by the network IGP's shortest path. A strict command is used to identify the path as the ERO and a loose command is used for the CSPF algorithm. When implementing a link protection using FFR, it is advisable to use ERO since the CSPF will re-optimize the network in case of a link failure by recalculating the primary link instead of using the backup tunnel, unless re-optimization is disabled. This makes the network behaviour unpredictable.

As can be seen in listing 1, nodes are represented by the last value of the prefix. For example for node N20 it is 10.123.100.20. The FFR protection is configured with one-to-one. Because of the ERO, the primary path is set to N12-N20-N22 and re-optimization is disabled. Links N12-N20 and N20-N22 are both protected. The protection configurations are needed only on the ingress LSR because the protection is unidirectional just as it is the case for LSPs. The ingress LSR then transmits information to the respective LSRs about the protection. Also in listing 1 the reroute source and destination are also shown as well as the mapped route.

6.3 Link Protection Verification

In an MPLS network it is possible for the network to reuse the same label across the network. In the implementation different labels were used to distinguish the labels between different links. Monitory command was used to verify the link protection configured. The show RSVP session in listing 2 below shows there are two RSVPs, the Ingress RSVP and the Transit RSVP.

```
N12# show rsvp session

Ingress RSVP:

To              From            State   Type  ETI             TID   LID   Labelin Labelout   Name
10.123.100.22   10.123.100.12   Up      Pri   10.123.100.12   1     2     -       87040      N12toN22_Forward_Tunnel
10.123.100.22   10.123.100.12   Up      Pde   10.123.100.12   1     2     -       87050      N12toN22_Forward_Tunnel
Total 2 displayed, Up 2, Down 0.


Transit RSVP:

To              From            State   Type  ETI             TID   LID   Labelin Labelout   Name
10.123.100.22   10.123.100.12   Up            0.123.100.12    1     2     87045   87040      N12toN22_Forward_Tunnel
Total 1 displayed, Up 1, Down 0.
```

Listing 2. RSVP session in N12.

The Ingress LSP RSVP has a primary tunnel (Pri) and a primary detour (Pde). The primary tunnel is N12-N22 through N20. The label from N12 to N20 is 87040. The primary tunnel is used when the network is working normally. The primary detour is used when the link N12-N20 fails. During a normal network operation, it can be used to transmit low priority data. The primary detour tunnel is N12-N22 through N14 and N18. The label from N12 to N14 is 87050. The status of both the tunnels have to be up thus giving an indication that they are configured right and are ready to forward MPLS packets.

The transit tunnel is used when there is a failure on link N20-N22 and traffic has to be transmitted to N22 from N20 through the LSP N20-N12-N14-N18-N22. When N20-N22 link has failed, traffic from N12 will be transmitted to N20 and the label swapped and the packets forwarded with a different label back to N12. In N12 the label will be swapped again. The traffic will merge to join the backup tunnel. The incoming packets from N20 will have label 87045 and they will be forwarded with label 87050. In-depth

details can be seen in appendix 2, N12 RSVP session details. Figure 25 shows how the primary and backup tunnels have been created, the label expected for each LSP and the direction of the LSP.

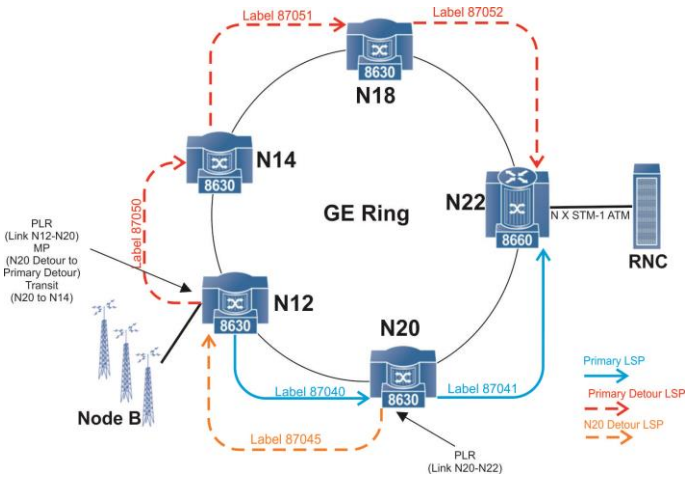

Figure 25. Label distribution in the implementation topology

As seen in figure 25, there are two points of local repair (PLR) on N20 for link N20-N22 and on N12 for link N12-N20. N12 is the merge point for transit traffic from N20 to the backup tunnel N12-N14-N18-N22. This traffic sees the primary detour as a primary LSP and merges to it.

Listing 3 below shows the MPLS packet labels. There are two tunnels, detour and transit LSPs. The detour is used only when the LSP N20-N22 fails, otherwise the packets use the transit LSP to N22.

```
N20#show rsvp session
Ingress RSVP:
To              From          State  Type  ETI             TID  LID  Labelin  Labelout  Name
10.123.100.22   10.123.100.12 Up     Det   10.123.100.12   1    2    -        87045     N12toN22_Forward_Tunnel
Total 1 displayed, Up 1, Down 0.

Transit RSVP:
To              From          State  Type  ETI             TID  LID  Labelin  Labelout  Name
10.123.100.22   10.123.100.12 Up           10.123.100.12   1    2    87040    87041     N12toN22_Forward_Tunnel
Total 1 displayed, Up 1, Down 0.
```

Listing 3. RSVP session in N20

Packets are forwarded to N22 though either the primary LSP or the backup LSP. Listing 4 below show both the primary and the backup LSPs. The status of both the LSPs has to be up when the network is working normally. The primary LSP's label is 87041 while the backup LSP's is 87052.

```
N22#show rsvp session
Egress RSVP:
To              From            State  Type  ETI             TID   LID  Labelin  Labelout  Name
10.123.100.22   10.123.100.12   Up          10.123.100.12   1     2    87041    -         N12toN22_Forward_Tunnel
10.123.100.22   10.123.100.12   Up          10.123.100.12   1     2    87052    -         N12toN22_Forward_Tunnel
Total 2 displayed, Up 2, Down 0.
```

Listing 4. RSVP session in N22

Appendix 3, N22 RSVP session details shows, in depth the forwarding of data to N22 through the two tunnels. The hop-by-hop usage of both of the tunnels can be seen in appendix 3. Only the links N12-N20 and N20-N22 are protected. This protection was configured only in N12 and the information transmitted to other LSRs in the network automatically with RSVP-TE FRR path messages.

6.4 Protection Scenario with a Link Failure

In the given topology there are two possible failure scenarios since only two links have protection. These scenarios are:

- Failure on link N12-N20
- Failure on link N20-N22.

Both of these scenarios were tested and the protection was able to protect the network from MPLS packets drop. The specific link was shut down to emulate a link failure.

6.5 Testing the LSP with Link N12-N20 Failure

The MPLS packets from N12 being sent to N22 use the LSP N12-N20-N22 when the network is working normally. Because of the FRR link protection configured in the ingress LSR, when the link fails, the traffic needs to be rerouted through the backup tunnel. Figure 26 below shows the route the traffic takes when there is a link failure on link N12-N20.

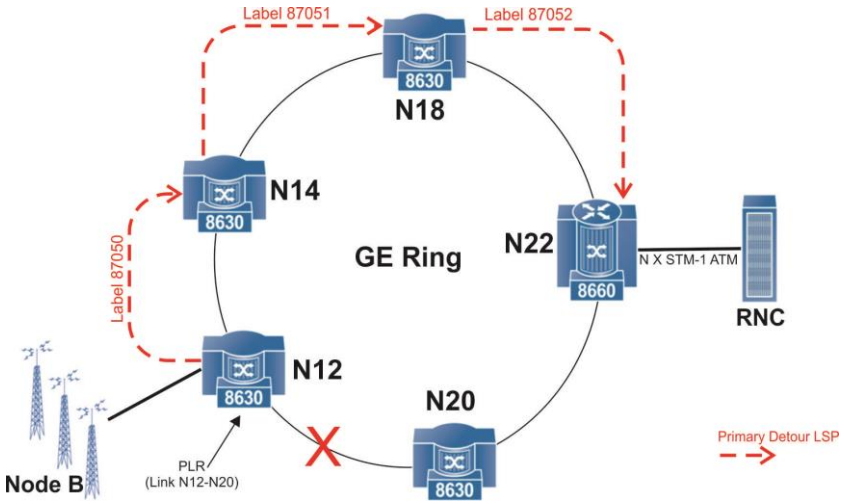

Figure 26. Network topology with a failure on link L12-N20.

As can be seen in figure 26, the only route to the egress LSR is through the LSP N12-N14-N18-N22. This can be seen using monitory commands or software. In this project monitory commands were used to trace the route taken by the packets. Listing 5 a) below shows the RSVP session status on LSR N12 before the link failure while listing 5 b) shows the RSVP session status after the link failure.

a) Before the link failure

```
N12#sh rsvp session

Ingress RSVP:

To              From          State  Type  ETI             TID  LID  Labelin  Labelout  Name
10.123.100.22   10.123.100.12 Up     Pri   10.123.100.12   1    2    -        87040     N12toN22_Forward_Tunnel
10.123.100.22   10.123.100.12 Up     Pde   10.123.100.12   1    2    -        87050     N12toN22_Forward_Tunnel
Total 2 displayed, Up 2, Down 0.


Transit RSVP:

To              From          State  Type  ETI             TID  LID  Labelin  Labelout  Name
10.123.100.22   10.123.100.12 Up           10.123.100.12   1    2    87045    87050     N12toN22_Forward_Tunnel
Total 1 displayed, Up 1, Down 0.
```

b) After the link failure

```
N12#show rsvp session

Ingress RSVP:

To              From          State       Type  ETI             TID  LID  Labelin  Labelout  Name
10.123.100.22   10.123.100.12 Using FRR   Pri   10.123.100.12   1    6    -        -         N12toN22_Forward_Tunnel
10.123.100.22   10.123.100.12 Up          Pde   10.123.100.12   1    6    -        87050     N12toN22_Forward_Tunnel
Total 2 displayed, Up 2, Down 0.


Transit RSVP:

To              From          State  Type  ETI             TID  LID  Labelin  Labelout  Name
10.123.100.22   10.123.100.12 Up           10.123.100.12   1    6    87045    87050     N12toN22_Forward_Tunnel
Total 1 displayed, Up 1, Down 0.
```

Listing 5. RSVP session on N12 before and after a link failure on link N12-N20.

Listing 5 above illustrates that the type of the primary (Pri) LSP changes once the link has failed and it indicates that FRR is in use. Since there is no link to N20 once the link N12-N20 has failed, there is no label to that LSR. FFR is used to fast reroute the traffic to the backup tunnel which eliminates data loss because of link N12-N20 failure.

6.6 Testing the LSP with Link N20-N22 Failure

The other possible scenario is when link N20-N22 fails. In this case the traffic will still be forwarded through the Primary link N12-N20 but on getting to LSR N20 the traffic will have to be routed back to N12 since the link to N22 has failed. N20 will be the point of local repair for the traffic from N12. The MPLS label will be swapped with another label in N20 and retransmitted to N12. N12 will be the merge point for the traffic from N20 headed for N22. Since there is already a primary backup tunnel on N12, the traffic will join this tunnel since it views it as a main LSP for the route to N22. Figure 27 below shows the route followed by the MPLS packet from Node B to the RNC with a failure on link N20-N22.

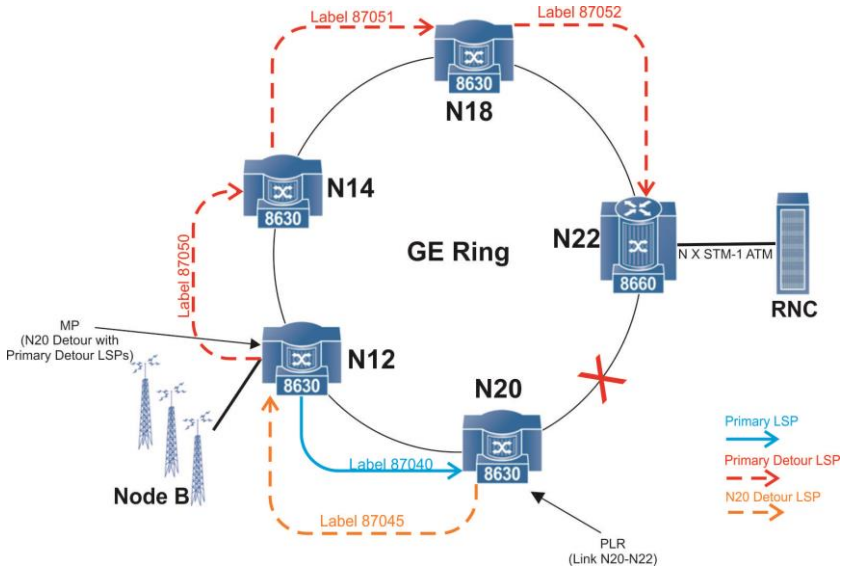

Figure 27. Network topology with a failure on link L20-N22.

Monitory commands were used to verify the changes in the traffic path in the network before and after link N20-N22 failed. It can be concluded from listing 6 a) below that the traffic getting to LSR N20 is using the LSR as a transit LSP since both the label in and label out are set on the MPLS packet. The detour (Det) link is not in use since the network is working normally. Once link N20-N22 fails, the label to N22 from N20 will be dropped, hence the traffic is forwarded through the backup tunnel. This can be conformed in listing 6 b) where there is only a label-in on the transit tunnel. The packets are transmitted back to N12 using the label 87045.

a) Before link failure

```
N20#show rsvp session

Ingress RSVP:

To              From            State   Type    ETI             TID   LID   Labelin   Labelout   Name

10.123.100.22   10.123.100.12   Up      Det     10.123.100.12   1     2     -         87045      N12toN22_Forward_Tunnel

Total 1 displayed, Up 1, Down 0.


Transit RSVP:

To              From            State   Type    ETI             TID   LID   Labelin   Labelout   Name

10.123.100.22   10.123.100.12   Up              10.123.100.12   1     2     87040     87041      N12toN22_Forward_Tunnel

Total 1 displayed, Up 1, Down 0.
```

b) After Link failure

```
N20#sh rsvp session

Ingress RSVP:

To              From            State   Type    ETI             TID   LID   Labelin   Labelout   Name

10.123.100.22   10.123.100.12   Up      Det     10.123.100.12   1     12    -         87045      N12toN22_Forward_Tunnel

Total 1 displayed, Up 1, Down 0.


Transit RSVP:

To              From            State       Type    ETI             TID   LID   Labelin   Labelout   Name

10.123.100.22   10.123.100.12   Using FRR           10.123.100.12   1     12    87040     -          N12toN22_Forward_Tunnel

Total 1 displayed, Up 1, Down 0.
```

Listing 6. RSVP session on N20 before and after a link failure on link N20-N22

In listing 6 b) above the state of the transit indicates that FFR is in use, thus meaning that traffic is being rerouted to a different tunnel and not using the transit tunnel. The only other tunnel in this topology from N20 is through N12. This is also verified in appendix 3 where the hop by hop of the traffic is shown on N22 when avoiding N22.

7 Conclusion

This project was set out to explore protection in MPLS-TE networks and focussed on link protection using FFR. The 1:1 protection scheme was used in the implementation with real network equipment at Tellabs Laboratory. The 1:1 protection scheme is one of four protection schemes available for MPLS protection. The other protection schemes are 1+1, N:1 and N:M. The MPLS protection can be divided into end-to-end and local protections. Local protection has both node and link protections.

In the project, a theoretical review of VPN, MPLS and traffic protection was carried out and documented. It shows the relationship between IP networks, VPN and MPLS. Different MPLS terminologies were learned from the study.

The goal of the project was achieved because the MPLS-TE was successfully implemented to support traffic protection using the FRR 1:1 scheme. An understanding of MPLS operation for the support of traffic protection was gained including related protocols such as VPN. The project implementation and testing were done and positive results were achieved which verify that MPLS-TE is efficient technology for traffic protection.

The aspiration now is to learn more about MPLS and spread the gained knowledge in real life as well as to carry out future study and implementation of other protection mechanisms in RSVP-TE enabled MPLS networks. Further research could be done to find the efficiency of different protection mechanisms, test rerouting duration and packet drop during the switchover using external test devices.

References

1 CenterSpan. Internet tutorial: What Is the internet? [online]. CenterSpan. URL: http://www.centerspan.org/tutorial/net.htm. Accessed 3rd December 2012.

2 TCP/IP Introduction. [online] W3Schools. Norway. URL: http://www.w3schools.com/tcpip/tcpip_intro.asp Accessed 3rd December 2012.

3 What is Leased Line? [online] DATANET.CO.UK Ltd. United Kingdom. URL: http://www.datanet.co.uk/leased_lines.aspx. Accessed 15th January 2012.

4 Alwary L. Advanced MPLS Design and Implementation. Indiana: cisco Press; 2001.

5 Fundamentals of Network Security Companion Guide. Indianapolis, USA: Cisco Press; 2004.

6 Watkins M, Wallace K. CCNA Security official exam certification guide. Indianapolis, USA: Cisco Press; 2008.

7 HOLBLink VPN. [online] HOB Secure Business Connectivity. Canada. URL: http://www.hobsoft.com/products/connect/VPN.jsp Accessed 14th January 2013.

8 Meeta G. Building a Virtual Private Network. Ohio, USA: Premier Press; 2003.

9 Virtual private network. [online] The Citizens' Compendium. URL: http://en.citizendium.org/wiki/Virtual_private_network Accessed 25th January 2013.

10 Lewis M. Comparing, Designing, and Deploying VPNs. Indianapolis, USA: Cisco Press; 2006.

11 Layer 3 VPNs (L3VPN) [online] Cisco Press. Indianapolis, USA. URL: http://www.cisco.com/en/US/products/ps6604/products_ios_protocol_ group_home.html Accessed 28th January 2013

12 Minei I, Lucek J. MPLS-Enabled Application: Emerging Developments and New Technologies (Third Edition). West Sussex, England: John Wiley & Sons; 2011.

13 Osborne E, Simha A. Traffic Engineering with MPLS. Indiana: Cisco Press; 2003.

14 Bisht S. Overlay, Peer-to-Peer and MPLS VPN [online] New Delhi, India. URL:http://networkshorizon.blogspot.fi/2012/01/overlay-peer-to-peer-and-mpls-vpn.html Accessed 29th January 2013.

15 IXIM. Multi-Protocol Label Switching (MPLS) Conformance and Performance Testing [ONLINE]. 2004.
URL: http://www.ixiacom.com/pdfs/library/white_papers/mpls.pdf.
Accessed 20th December 2012.

16 International Engineering Consortium. Multiprotocol Label Switching (MPLS) [ONLINE]. 2007.
URL: http://blinky-light.org/netroking/mpls.pdf
Accessed 20th December 2012.

17 Rosen EC, Viswanathan A, Callon R. Multiprotocol Labe Switching Architecture [ONLINE].
URL: http://tools.ietf.org/html/rfc3031.

18 Ghein LD. MPLS fundamentals. Indiana: Cisco Press; 2007.

19 Lee S, Griffith D, Coussot V, Su D. ER-LSP Setup for Multi-Service in Lambda Label Network [online]. Gaintherburg: national Institute of Standards and Technology; 2001.
URL: http://w3.antd.nist.gov/pubs/globecom2001.pdf.
Accessed 15th January 2013.

20 Configuring Multiprotocol BGP (MP-BGP) Support for CLNS [online]. Cisco Systems Inc; 2007.
URL: Http://www.cisco.com/en/US/docs/ios/12_2sr/12_2srb/feature/guide/brbclns.pdf
Accessed 20th January 2013.

21 Protocol Independent Multicast: [online] Creative Commons Attribution-ShareAlike License; 2012.
URL: http://en.wikipedia.org/wiki/Protocol_Independent_Multicast
Accessed 20th January 2013.

22 Label Distribution Protocol Extensions for Point-to-Multipoint and Multipoint-to-Multipoint Label Switched Paths [online]. Internet Engineering Task Force (IETF); 2011
URL: http://tools.ietf.org/html/rfc6388
Accessed 20th January 2013.

23 LDP Specification [online]. Internet Engineering Task Force (IETF); 2001
URL: http://www.rfc-editor.org/rfc/rfc3036.txt
Accessed 25th January 2013.

24 Overlay and Peer-to-Peer VPN Model. Softeware Defined Networking Summit Transformation Network Architecture. [online] eTutorials 2008-2012.
URL: http://etutorials.org/Networking/MPLS+VPN+Architectures/Part+2+MPLS-based+Virtual+Private+Networks/Chapter+7.+Virtual+Private+Network+VPN+Implementation+Options/Overlay+and+Peer-to-peer+VPN+Model/
Accessed 29th January 2013

25 Lancy L. MPLS configuration on Cisco IOS software. Indianapolis, USA: Cisco Press; 2005.

26 De Ghein L. MPLS Fundamentals. Indianapolis, USA: Cisco Press; 2007.

27 Balliache L. LDP Operation (online).
URL: http://opalsoft.net/qos/MPLS-42.htm
Accessed 5th February 2013

28 Cisco Nexus 700 series NX-OS MPLS Configuration Guide. Indianapolis, USA: Cisco Press; 2012.

29 Configuring MPLS RSVP TE. (online). Indianapolis, USA:Cisco Press
URL: http://www.cisco.com/en/US/docs/switches/datacenter/sw/5_x/nx-os/mpls/configuration/guide/mp_te_RSVP.pdf

Appendix 1. N12 RSVP session detail

N12#show rsvp session detail
Ingress (Primary)
10.123.100.22
From: 10.123.100.12, LSPstate: Up, LSPname: N12toN22_Forward_Tunnel
Setup priority: 7, Hold priority: 0
CSPF usage: Enabled, CSPF type: OSPF, CSPF Retry Count: 0, CSPF Retry Interval: 30 seconds
CSPF metric: 100
Reoptimization: disabled
FRR Mode: one-to-one
Recovery mode: reoptimize
Status: LSP fully protected
Label in: -, Label out: 87040,
Tspec rate: 0, Fspec rate: 0
Tunnel Id: 1, LSP Id: 2, Ext-Tunnel Id: 10.123.100.12
Downstream: 10.12.20.20, ge9/0/7
Path refresh: 30 seconds (due in 21 seconds)
Resv lifetime: 157 seconds (due in 148 seconds)
Retry count: 0, intrvl: 30 seconds
RRO re-use as ERO: Disabled
Label Recording: Enabled
Admin Groups: none
Configured Path: N12toN22_Forward_Tunnel_Path (in use)
Configured Explicit Route Detail :
10.123.100.22/32 loose
Session Explicit Route Detail :
10.12.20.20/32 strict
10.20.22.22/32 strict
Record route:
<self> link protected
10.123.100.20 link protected node-id 87040
10.12.20.20 link protected 87040
10.123.100.22 no protection node-id 87041

10.20.22.22 no protection 87041
Style: Shared Explicit Filter
Traffic type: controlled-load
Minimum Path MTU: 1500
QoS Reservation Reference Count: 1
LSP Type: ELSP_CONFIG
DSTE Class Type Number: 0, Class Type name: best_effort
Uptime: 00:09:40, Total uptime: 00:09:40, First up: 00:09:40 ago
State transitions: 1
Ingress FSM state: Operational
Wait to restore: 0 ms, wait to use: 0 ms, wait before MBB: 1000 ms
Wait before deleting pre-MBB session: 1000 ms
Last Recorded Error Code: None
Last Recorded Error Value: None
Node where Last Recorded Error originated: None
Previous Recorded Error Code: Ingress Problem (1000)
Previous Recorded Error Value: Egress configuration error (2)
Node where Previous Recorded Error originated: self
Output statistics (updated 00:00:00 ago):
Bytes 0, packets 0, errors 0
Interval statistics:
1 min: bit rate 0 b/s packet rate 0 pkt/s

Transit
10.123.100.22
From: 10.123.100.12, LSPstate: Up, LSPname: N12toN22_Forward_Tunnel
Setup priority: 7, Hold priority: 0
FRR Mode: None
Merged to: local detour, from 10.123.100.12
Detour object:
10.123.100.20 avoiding 10.20.22.22
Label in: 87045, Label out: 87050,
Tspec rate: 0, Fspec rate: 0
Tunnel Id: 1, LSP Id: 2, Ext-Tunnel Id: 10.123.100.12
Downstream: 10.12.14.14, ge9/0/6 Upstream: 10.12.20.20, ge9/0/7

Path lifetime: 157 seconds (due in 129 seconds)
Resv refresh: 30 seconds (due in 26 seconds)
Resv lifetime: 157 seconds (due in 132 seconds)
RRO re-use as ERO: Disabled
Label Recording: Enabled
Admin Groups: none
Received Explicit Route Detail :
10.12.20.12/32 strict
10.12.14.14/32 strict
10.14.18.18/32 strict
10.18.22.22/32 strict
Session Explicit Route Detail :
10.12.14.14/32 strict
10.14.18.18/32 strict
10.18.22.22/32 strict
Record route:
10.12.20.20 no protection 87040
10.123.100.20 no protection node-id 87040
<self> no protection
10.123.100.14 no protection node-id 87050
10.12.14.14 no protection 87050
10.123.100.18 no protection node-id 87051
10.14.18.18 no protection 87051
10.123.100.22 no protection node-id 87052
10.18.22.22 no protection 87052
Style: Shared Explicit Filter
Traffic type: controlled-load
Minimum Path MTU: 1500
QoS Reservation Reference Count: 2
LSP Type: ELSP_CONFIG
DSTE Class Type Number: 0, Class Type name: best_effort
Blacklist:N/A,
Uptime: 00:09:20, Total uptime: 00:09:20, First up: 00:09:20 ago
State transitions: 1
Transit upstream state: Operational, downstream state: Operational

Last Recorded Error Code: None
Last Recorded Error Value: None
Node where Last Recorded Error originated: None
Previous Recorded Error Code: None
Previous Recorded Error Value: None
Node where Previous Recorded Error originated: None

Ingress (Primary detour)
10.123.100.22
From: 10.123.100.12, LSPstate: Up, LSPname: N12toN22_Forward_Tunnel
Setup priority: 7, Hold priority: 0
CSPF usage: Enabled, CSPF type: OSPF, CSPF Retry Count: 0, CSPF Retry Interval: 30 seconds
CSPF metric: 150
Reoptimization: disabled
FRR Mode: None
Detour object:
10.123.100.12 avoiding 10.12.20.20
Merged detour objects:
10.123.100.20 avoiding 10.20.22.22
Label in: -, Label out: 87050,
Tspec rate: 0, Fspec rate: 0
Tunnel Id: 1, LSP Id: 2, Ext-Tunnel Id: 10.123.100.12
Downstream: 10.12.14.14, ge9/0/6
Path refresh: 30 seconds (due in 6 seconds)
Resv lifetime: 157 seconds (due in 132 seconds)
Retry count: 0, intrvl: 30 seconds
RRO re-use as ERO: Disabled
Label Recording: Enabled
Admin Groups: none
Configured Path: none
Session Explicit Route Detail :
10.12.14.14/32 strict
10.14.18.18/32 strict
10.18.22.22/32 strict

Record route:
<self> no protection
10.123.100.14 no protection node-id 87050
10.12.14.14 no protection 87050
10.123.100.18 no protection node-id 87051
10.14.18.18 no protection 87051
10.123.100.22 no protection node-id 87052
10.18.22.22 no protection 87052
Style: Shared Explicit Filter
Traffic type: controlled-load
Minimum Path MTU: 1500
QoS Reservation Reference Count: 2
LSP Type: ELSP_CONFIG
DSTE Class Type Number: 0, Class Type name: best_effort
Uptime: 00:09:40, Total uptime: 00:09:40, First up: 00:09:40 ago
State transitions: 1
Ingress FSM state: Operational
Wait to restore: 0 ms, wait to use: 0 ms, wait before MBB: 1000 ms
Wait before deleting pre-MBB session: 1000 ms
Last Recorded Error Code: None
Last Recorded Error Value: None
Node where Last Recorded Error originated: None
Previous Recorded Error Code: Ingress Problem (1000)
Previous Recorded Error Value: Egress configuration error (2)
Node where Previous Recorded Error originated: self

Appendix 2. N20 RSVP session details

```
N20#show rsvp session detail
Transit
10.123.100.22
  From: 10.123.100.12, LSPstate: Up, LSPname: N12toN22_Forward_Tunnel
  Setup priority: 7, Hold priority: 0
  FRR Mode: one-to-one
  Label in: 87040,  Label out: 87041,
  Tspec rate: 0, Fspec rate: 0
  Tunnel Id: 1, LSP Id: 2, Ext-Tunnel Id: 10.123.100.12
  Downstream: 10.20.22.22, ge9/0/6   Upstream: 10.12.20.12, ge9/0/7
  Path refresh: 30 seconds (due in 34 seconds)
  Path lifetime: 157 seconds (due in 157 seconds)
  Resv refresh: 30 seconds (due in 8 seconds)
  Resv lifetime: 157 seconds (due in 148 seconds)
  RRO re-use as ERO: Disabled
  Label Recording: Enabled
  Admin Groups: none
  Received Explicit Route Detail :
   10.12.20.20/32 strict
   10.20.22.22/32 strict
  Session Explicit Route Detail :
   10.20.22.22/32 strict
  Record route:
   10.12.20.12       link protected                87040
   10.123.100.12     link protected           node-id 87040
   <self>            link protected
   10.123.100.22     no protection            node-id 87041
   10.20.22.22       no protection                 87041
  Style: Shared Explicit Filter
  Traffic type: controlled-load
  Minimum Path MTU: 1500
  QoS Reservation Reference Count: 1
  LSP Type:  ELSP_CONFIG
```

DSTE Class Type Number: 0, Class Type name: best_effort
Blacklist:N/A,
Uptime: 00:15:14, Total uptime: 00:15:14, First up: 00:15:14 ago
State transitions: 1
Transit upstream state: Operational, downstream state: Operational
Last Recorded Error Code: None
Last Recorded Error Value: None
Node where Last Recorded Error originated: None
Previous Recorded Error Code: None
Previous Recorded Error Value: None
Node where Previous Recorded Error originated: None

Ingress (Detour)
10.123.100.22
From: 10.123.100.12, LSPstate: Up, LSPname: N12toN22_Forward_Tunnel
Setup priority: 7, Hold priority: 0
CSPF usage: Enabled, CSPF type: OSPF, CSPF Retry Count: 0, CSPF Retry Interval: 30 seconds
CSPF metric: 200
Reoptimization: disabled
FRR Mode: None
Detour object:
10.123.100.20 avoiding 10.20.22.22
Label in: -, Label out: 87045,
Tspec rate: 0, Fspec rate: 0
Tunnel Id: 1, LSP Id: 2, Ext-Tunnel Id: 10.123.100.12
Downstream: 10.12.20.12, ge9/0/7
Path refresh: 30 seconds (due in 40 seconds)
Resv lifetime: 157 seconds (due in 132 seconds)
Retry count: 0, intrvl: 30 seconds
RRO re-use as ERO: Disabled
Label Recording: Enabled
Admin Groups: none
Configured Path: none
Session Explicit Route Detail :

10.12.20.12/32 strict
10.12.14.14/32 strict
10.14.18.18/32 strict
10.18.22.22/32 strict
Record route:
<self> no protection
10.123.100.12 no protection node-id 87050
10.12.20.12 no protection 87050
10.123.100.14 no protection node-id 87051
10.12.14.14 no protection 87051
10.123.100.18 no protection node-id 87052
10.14.18.18 no protection 87052
10.123.100.22 no protection node-id 87052
10.18.22.22 no protection 87052
Style: Shared Explicit Filter
Traffic type: controlled-load
Minimum Path MTU: 1500
QoS Reservation Reference Count: 1
LSP Type: ELSP_CONFIG
DSTE Class Type Number: 0, Class Type name: best_effort
Uptime: 00:14:53, Total uptime: 00:14:53, First up: 00:14:53 ago
State transitions: 1
Ingress FSM state: Operational
Wait to restore: 0 ms, wait to use: 0 ms, wait before MBB: 1000 ms
Wait before deleting pre-MBB session: 1000 ms
Last Recorded Error Code: None
Last Recorded Error Value: None
Node where Last Recorded Error originated: None
Previous Recorded Error Code: Ingress Problem (1000)
Previous Recorded Error Value: Egress configuration error (2)
Node where Previous Recorded Error originated: self

Appendix 2. N22 RSVP session details

```
N22#show rsvp session detail
Egress
10.123.100.22
  From: 10.123.100.12, LSPstate: Up, LSPname: N12toN22_Forward_Tunnel
  Setup priority: 7, Hold priority: 0
  FRR Mode: one-to-one
  Label in: 87041,  Label out: -,
  Tspec rate: 0, Fspec rate: 0
  Tunnel Id: 1, LSP Id: 2, Ext-Tunnel Id: 10.123.100.12
  Upstream: 10.20.22.20, ge13/0/7
  Path lifetime: 157 seconds (due in 153 seconds)
  Resv refresh: 30 seconds (due in 10 seconds)
  RRO re-use as ERO: Disabled
  Label Recording: Enabled
  Admin Groups: none
  Received Explicit Route Detail:
   10.20.22.22/32 strict
  Record route:
   10.12.20.12       link protected                87040
   10.123.100.12     link protected           node-id 87040
   10.20.22.20       link protected                87041
   10.123.100.20     link protected           node-id 87041
   <self>            no protection
  Style: Shared Explicit Filter
  Traffic type: controlled-load
  Minimum Path MTU: 1500
  QoS Reservation Reference Count: 1
  LSP Type:  ELSP_CONFIG
  DSTE Class Type Number: 0, Class Type name: best_effort
  Blacklist:N/A,
  Uptime: 00:17:19, Total uptime: 00:17:19, First up: 00:17:19 ago
  State transitions: 1
  Egress FSM state: Operational
```

Last Recorded Error Code: None
Last Recorded Error Value: None
Node where Last Recorded Error originated: None
Previous Recorded Error Code: None
Previous Recorded Error Value: None
Node where Previous Recorded Error originated: None

Egress
10.123.100.22
From: 10.123.100.12, LSPstate: Up, LSPname: N12toN22_Forward_Tunnel
Setup priority: 7, Hold priority: 0
FRR Mode: None
Detour object:
10.123.100.12 avoiding 10.12.20.20
10.123.100.20 avoiding 10.20.22.22
Label in: 87042, Label out: -,
Tspec rate: 0, Fspec rate: 0
Tunnel Id: 1, LSP Id: 2, Ext-Tunnel Id: 10.123.100.12
Upstream: 10.18.22.18, ge13/0/6
Path lifetime: 157 seconds (due in 152 seconds)
Resv refresh: 30 seconds (due in 8 seconds)
RRO re-use as ERO: Disabled
Label Recording: Enabled
Admin Groups: none
Received Explicit Route Detail :
10.18.22.22/32 strict
Record route:
10.12.14.12 no protection 87050
10.123.100.12 no protection node-id 87050
10.14.18.14 no protection 87051
10.123.100.14 no protection node-id 87051
10.18.22.18 no protection 87052
10.123.100.18 no protection node-id 87052
<self> no protection
Style: Shared Explicit Filter

Traffic type: controlled-load
Minimum Path MTU: 1500
QoS Reservation Reference Count: 1
LSP Type: ELSP_CONFIG
DSTE Class Type Number: 0, Class Type name: best_effort
Blacklist:N/A,
Uptime: 00:17:18, Total uptime: 00:17:18, First up: 00:17:18 ago
State transitions: 1
Egress FSM state: Operational
Last Recorded Error Code: None
Last Recorded Error Value: None
Node where Last Recorded Error originated: None
Previous Recorded Error Code: None
Previous Recorded Error Value: None
Node where Previous Recorded Error originated: None